COLUMBIA LAW SCHOOL

PUBLIC LAW & LEGAL THEORY WORKING PAPER GROUP

PAPER NUMBER 14-412

IN DEFENSE OF THE PANOPTICON

WILLIAM H. SIMON

OCTOBER 2014

Boston Review
Sept-Oct. 2014

IN DEFENSE OF THE PANOPTICON

William H. Simon

Anxiety about surveillance and data mining has led many to embrace implausibly expansive and rigid conceptions of privacy. Activists seem to have lost touch with the reservations about privacy expressed in the social criticism of some decades ago. They seem unable to imagine that pre-occupation with privacy might amount to a "pursuit of loneliness" or that "eyes on the street" might have reassuring connotations. Without denying the importance of the effort to define and secure privacy values, I want to catalogue and push back against some key rhetorical tropes that distort current discussion and practice.

One problem is that privacy defenses often imply a degree of pessimism about the state that is inconsistent with the strong general public regulatory and social-welfare role that many defenders favor. Another is a sentimental disposition toward past convention that obscures the potential contributions of new technologies to both order and justice. And a third is a narrow conception of personality that exalts extreme individual control over information at the expense of sharing and sociability.

I. Paranoia

In urban areas, most people's activity outdoors and in the common spaces of buildings is recorded most of the time. Surveillance cameras are everywhere. When people move around, their paths are registered on building access cards or subway fare cards or automobile toll devices. Their telephone and e-mail communications, internet searches, and movements are tracked by telephone companies and other intermediaries. All their credit card transactions – which for many people, means nearly all of their

transactions -- are documented by time, place, and substance. The health system extracts and records detailed information about their psychic and bodily functions. Anyone arrested, and many who fear arrest, in the criminal justice system typically surrender a variety of personal information and often have to submit to ongoing monitoring. Even within the home, water and energy consumption is monitored, and some people choose to install cameras to monitor children or protect against burglars.

To many people, this society looks like the Panopticon – a prison designed as a circular tower so that the inmates can be easily observed by a centrally located authority figure. Jeremy Bentham originated the Panopticon idea as a low-cost form of subjugation for convicted criminals. Michel Foucault adopted it as a metaphor for what he regarded as the insidiously pervasive forms of social control in contemporary society. To him, schools, hospitals, workplaces, and government agencies all engaged in repressive forms of surveillance analogous to the Panopticon.

In the United States, paranoid political style has been associated traditionally with the right and the less educated. But Foucault helped made it attractive to liberal intellectuals. His contribution was largely a matter of style. Foucault was the most moralistic of social theorists, but he purported to disdain morality ("normativity") and refused to acknowledge, much less defend, the moral implications of his arguments. He gave intellectual respectability to the three principal tropes of the paranoid style.

First, there is the idea of guilt by association. The resemblance between some feature of a strikingly cruel or crackpot regime of the past or in fiction (especially in *1984*) and a more ambiguous contemporary one is emphasized in order to condemn the latter. Thus, the elaborate individualized calibration of tortures in 18th and 19th century penology is used to make us feel uncomfortable about the graduated responses to noncompliance in contemporary drug treatment courts. Orwell's image of television cameras transmitting images from inside the home to the political police is used to induce anxiety about devices that monitor electricity usage so that the hot water tank will re-heat during off-peak hours.

The second trope of the paranoid style is the portrayal of virtually all tacit social pressure as insidious. What people experience as voluntary choice is substantially conditioned by unconscious internalized dispositions to conform to norms, and a key mechanism of such conformity is the actual, imagined, or anticipated gaze of others. Almost everyone who thinks about it recognizes that such pressures are potentially benign, but people differ in their rhetorical predispositions toward them. The individualist streak in American culture tends to exalt individual choice in a way that makes social influence suspect.

Foucault disdained individualism, but he introduced a conception of "power" that was so vague and sinister that it could be applied to make almost any social force seem creepy. When Neil Richards writes in the Harvard Law Review that surveillance "affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance," he is channeling Foucault. So is Julie Cohen, when she writes in the Stanford Law Review: "Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."

We have come a far cry from Jane Jacobs's idea of "eyes on the street" as the critical foundation of urban vibrancy. For Jacobs, the experience of being observed by diverse strangers induces, not anxiety or timidity, but an empowering sense of security and stimulation. It makes people willing to go out into new situations and to experiment with new behaviors. Eyes-on-the-street implies a tacit social pact that people will intervene to protect each other's safety but that they will refrain from judging their peers' non-dangerous behavior. Electronic surveillance is not precisely the same thing as Jacobean eyes-on-the-street, but it does offer the combination of potentially benign intervention and the absence of censorious judgment that Jacobs saw as conducive to autonomy.

The third trope of the paranoid style is the "slippery slope" argument. The idea is that an innocuous step in a feared direction will inexorably lead to further steps that end in catastrophe. As *The Music Man* puts it in explaining why a pool table will lead to

moral collapse in River City, Iowa, "medicinal wine from a teaspoon, then beer from a bottle." In this spirit, Daniel Solove in *Nothing to Hide* explains why broad surveillance is a threat even when limited to detection of unlawful activity: First, surveillance will sometimes lead to mistaken conclusions that will harm innocent people. Second, since "everyone violates the law sometimes" (think of moderate speeding on the highway), surveillance will lead to over-enforcement of low-stakes laws (presumably by lowering the costs of enforcement), or perhaps the use of threats of enforcement of minor misconduct to force people to give up rights (as for example, where police threaten to bring unrelated charges in order to induce a witness or co-conspirator to cooperate in the prosecution of another). And finally, even if we authorize broad surveillance for legitimate purposes, officials will use the authorization as an excuse to extend their activities in illegitimate ways.

Yet, "slippery slope" arguments can be made against virtually any kind of law enforcement. Most law enforcement infringes privacy. ("Murder is the most private act a man can commit," William Faulkner wrote.) And most law enforcement powers have the potential for abuse. What we can reasonably ask is, first, that the practices are calibrated effectively to identify wrongdoers; second, that the burden they put on law-abiding people is fairly distributed; and third, that officials are accountable for the lawfulness of their conduct both in designing and in implementing the practices.

The capacity of broad-based electronic surveillance that collects data on large or indeterminate numbers of people who are not identified in advance to satisfy these conditions is in some respects higher than that of the more targeted and reactive approaches that privacy advocates prefer. Targeted approaches rely heavily on personal observation by police and witnesses, reports by informants of self-inculpatory statements by suspects, and confessions. Scholars in recent years have emphasized the fallibility of human memory and observation: Witness reports of conduct by strangers are often mistaken and influenced by investigators. Those who report self-inculpatory statements often

have dubious motivations, and, with surprising frequency, even confessions prove unreliable.

Inferences from broad-based electronic surveillance are not infallible, but they are often more reliable than reports of personal observation, and they can be less intrusive. Computers programmed to identify and photograph red light violations make much more reliable determinations of the violation than a police officer relying on his own observation. And they are less intrusive: the camera can be set to record only when there's a violation, whereas a police officer would observe and remember much more. Yet, many civil libertarians, including some ACLU affiliates, oppose them. One of their key arguments is that the systems generate tickets in many situations where the driver might have had an excuse for not stopping in time that would have persuaded a police officer to excuse the violation. (The case for excuse can still be made in court, but a court appearance would cost more than the ticket for many.) The argument is not frivolous, but it is a curiousity typical of this field that people concerned about the abuse of state power oppose new technology in favor of procedures that give officials more discretion.

For democratic accountability, Panopticon-style surveillance has an under-appreciated advantage. It may more easily accommodate transparency. Electronic surveillance is governed by fully specified algorithms. Thus, disclosure of the algorithms gives a full picture of the practices. By contrast, when government agents are told to scan for suspicious behavior, we know very little about what criteria they are using. Even if we require the agents to articulate their criteria, they may be unable to do so comprehensively. The concern is not just about good faith, but also about unconscious predisposition. Psychologists have provided extensive evidence of pervasive, unconscious bias based on race and other social stereotypes and stigma. Algorithm-governed electronic surveillance has no such bias.

The Panopticon can be developed in ways Foucault never imagined to discipline the watchers as well as the watched. The most vocal demands for electronic surveillance in prisons these days come from prisoners and their advocates. Lawsuits

challenging physical abuse by guards often produce court orders requiring increased deployment of video cameras and restricting guards' ability to take prisoners to areas where they are not recorded. People who worry about coerced confessions favor mandatory taping of police interviews of suspects, and many jurisdictions have adopted this practice. One response to complaints of racial profiling in pedestrian or vehicle stops has been to have police wear cameras that tape every encounter. Some civil libertarians oppose such practices, but those who favor them are trying to restrain state power, not enlarge it.

More generally, broad-reach electronic mechanisms have an advantage in addressing the danger that surveillance will be unfairly concentrated on particular groups. Targeting criteria, rather than reflecting rigorous efforts to identify wrongdoers, may reflect cognitive bias or group animus. Moreover, even when the criteria are optimally calculated to identify wrongdoers, they may be unfair to law-abiding people who happen to share some superficial characteristic with wrongdoers. Thus, law-abiding blacks complain that they are unfairly burdened by stop-and-frisk tactics, and law-abiding Muslims make similar complaints about anti-terrorism surveillance.

Such problems are more tractable with broad-based electronic surveillance. Because it is broad-based, it distributes some of its burdens widely. This may be intrinsically fairer, and it operates as a political safeguard, making effective protest more likely in cases of abuse. Because it is electronic, the efficacy of the criteria can be more easily investigated, and their effect on law-abiding people can be more accurately documented. Thus, plaintiffs in challenges to stop-and-frisk practices analyze electronically recorded data on racial incidence and "hit rates" to argue that the criteria are biased and the effects racially skewed. Remedies in such cases typically require more extensive recording.

The critics' pre-occupation with the dangers of state oppression often leads them to overlook the dangers of private surveillance. The critics have a surprisingly difficult time coming up with actual examples of serious harm from government

surveillance abuse. Instead, they tend to talk about the "chilling effect" from awareness of surveillance.

By contrast, there have been many examples of serious harm from private abuse of personal information gained from digital sources. At least one person has committed suicide as a consequence of the internet publication of video showing him engaged in sexual activity. Many people have been humiliated by private recording and publication of intimate conduct, and blackmail based on threats of such disclosure has emerged as a common practice. Some of this private abuse is and should be illegal. But the legal prohibitions can only be enforced if the government has some of the surveillance capacities that critics decry. It must be able to identify the wrongdoers and sanction their misconduct. Less compromising critics would deny government these capacities.

With falling crime rates and small risks of terrorism in the United States, privacy advocates do not feel compelled to address the potential chilling effect on speech and conduct that arises from fear of private lawlessness, but we do not have to look far to see examples of such an effect abroad and to recognize that its magnitude depends on the effectiveness of public law enforcement. To the extent that law enforcement is enhanced by surveillance, we ought to recognize the possibility of a "warming effect" that strengthens people's confidence that they can act and speak without fear of private aggression.

II. Nostalgia

Harm from surveillance that intrudes on core areas of solitude and intimacy is easy to identify. Such intrusion is rightly subject to high burdens of justification. But most surveillance is different. Often it involves conduct subject to ordinary observation in public or information that a person has willingly provided to strangers, often to facilitate business or commercial dealings.

Once we go beyond the solitary-intimate realm, it becomes harder to delimit the scope of privacy concerns. A common approach is to privilege assumptions based on past

experience. Thus, the Supreme Court elaborates the constitutional prohibition of "unreasonable searches and seizures" by looking to "expectations of privacy." Expectations are a function of custom. It follows that telescopically-aided airplane surveillance of someone in his backyard is generally OK because we are used to telescopes and airplanes flying over. Using thermal imaging technology to look inside the house requires a warrant because it is a technology to which we are not yet habituated. Helen Nissenbaum, in her highly-regarded *Privacy in Context*, takes a similar approach. Her guiding principle is "contextual integrity," which means the implicit customary norms in any given sphere of activity. If a highway toll collector sees contraband in the backseat of a car, that's not a problem because such observation is familiar. But if the police examine electronic toll records to see if the car was near the scene of a crime at the relevant time, that's a privacy problem.

Here again we see people of generally liberal views resorting to conservative rhetorical and theoretical tropes when it comes to privacy. Most privacy advocates probably consider the appeal to custom in arguments about the death penalty or gay marriage as a sign of intellectual bankruptcy. The distinctions that the customary principle produces seem arbitrary in relation to any substantive conception of privacy.

The substantive conception to which the advocates are most drawn is the notion of a right to control information about one's self. James Whitman argues in the *Yale Law Journal* that this conception evolved through the democratization of aristocratic values. The aristocrat's sense of self-worth and dignity depended on respect from peers and deference from subordinates, and both were a function of his public image. Image was thus treated as a kind of personal property. Whitman says this view continues to influence the European middle class in the age of equal citizenship. As the ideal was democratized, it came to be seen as a foundation for self-expression and individual development.

European law evolved to express this cultural change. Whitman showed that the idea of a right to control one's public image underlies French and German privacy law, and it appears to

animate European Union privacy law, which advocates admire for its stronger protections than those of US law. For example, French and German law impose stricter limits on credit reporting and the use of consumer data than US law. The EU directive mandates that individuals be given notice of the data collection practices of those with whom they deal and rights to correct erroneous data about them. More controversially, a proposed revision prohibits decisions based "solely on automatic data processing" for various purposes, including employment and credit. By contrast, US law tends to be less protective and less general. Its privacy law tends to be sectoral, with distinctive regulations for health care, education, law enforcement, and other fields.

Whitman associates the weaker influence of the idea of personal image-control in the US with the stronger influence here of competing libertarian notions that broadly protect speech and publication. Expansive notions of privacy require a more active state to enforce them. This was recently illustrated by a decision of the EU Court of Justice holding that the "right to be forgotten" may require removal from an internet website of true but "no longer relevant" information about the plaintiff's default on a debt. The prospect of courts reviewing internet data to determine when personal information is "no longer relevant" has emphasized the potential conflict between privacy and other civil rights.

But reservations about the broad conception of dignity Whitman describes go deeper. There is a powerful *moral* objection to it grounded in ideals of sociability. Even in Europe, during the period in which the ideal was democratized, there was a prominent critique of it. A character in a 19th century English novel pre-occupied with controlling his public image is likely to be a charlatan or a loser. Not for nothing is Sherlock Holmes the most prominent hero in the canon. His talents are devoted to invading the privacy of those who would use their image-management rights to exploit others. And as he teaches that the façade of self-presentation can be penetrated by observation and analysis of such matters as frayed cuffs, scratches on a watch, or a halting gait, he sets up as a competing value the capacity to know and deal with people on our terms as well as theirs.

Even among innocuous characters, pre-occupation with image control often appears as a pathology that inhibits rather than enhances self-expression and development. This pre-occupation is associated with a rejection of urban life and its spontaneity and diversity. Think of Sir Leicester Dedlock in *Bleak House* and Sir Walter Elliot in *Persuasion*, minor nobles clinging to aristocratic ideals. They know that the best way to maintain control of your image is to avoid contact with strangers, people you have no power over, and clever people who might penetrate your disguises. To embrace the vitality of the city requires a willingness to give up some control over one's image and accept risks of being understood and dealt with on terms that are not your own. In both books, the unwillingness to run these risks is associated with personal stultification.

If the right to control personal information was extended in Europe from the aristocracy to the rest of the society, it was at the same time diluted for everyone. When Darcy leaves his estate at Pemberley, he exits a world in which he is "seen as he chooses to be seen," as the scoundrel Wickham puts it enviously. In the middle class world of Meryton, he is subjected to eavesdropping and gossip (the social media of yesteryear). And he is confronted by people, notably Lizzie Bennet, who dare to "read [his] character" back to him in their own manner. In the process of responding, he grows and finds romantic fulfillment but only by giving up control. *Pride and Prejudice*, perhaps the most popular novel written in English, is a treatise on the impossibility and undesirability of giving anyone control over the information about himself.

As there are emotional and social benefits to giving up control over personal information; so are there are economic benefits. It is not unfair to take account of people's credit histories in making loan decisions. When lenders do this effectively, credit is, on average, cheaper. Nor does it seem especially unfair to take account of a factor like the purchase of home safety devices that predicts relevant behavior like repayment of a loan. Some uses of

personal information should be prohibited. Where predictive information tracks axes of historical subordination, such as race and gender, there may be good reason to limit its use, as the law does with respect to various insurance decisions. The reason, however, has to do with concerns about subordination, not some broad right of privacy. The US sectoral approach is better equipped to take account of the varying and competing stakes than the EU categorical one.

III. Individualism

A major goal of many privacy proponents is to limit collection of personal data either by regulations requiring affirmative consent for such collection or by technology that limits reading or retaining the data. They don't want, for example, Google to be able to analyze people's Internet searches or state governments to be able to analyze highway toll payment data without specific consent, or perhaps a warrant. They also advocate technologies such as the hardware-software package offered by the Freedom Box Foundation designed to enable users to thwart mining of their data over the Internet.

Advocates object most strongly to data collection designed to yield specific conclusions about the individual, but they persist even when anonymized data is used to assess general patterns. Since anonymization is never perfectly secure, there remains some risk to the subjects. Moreover, the privacy norm sometimes shades into a property norm. It turns out that some people carry around economically valuable information in their bodies – for example, the DNA code for a substance with therapeutic potential -- and that information about everyone's conduct and physical condition can, when aggregated, be sold for substantial sums. For some, the extraction of such information without consent looks like expropriation of property. They would like to see explicit recognition of property rights to personal information that could not be infringed without consent and

compensation. In Who Owns the Future? Jaron Lanier develops this line of thought, suggesting that we create institutions that enable individuals to "monetize" their personal data—individual accounts would be credited every time a piece of data is used.

In addressing such issues, a lot depends on how we understand "consent." Consent can mean clicking on an "I agree to the terms" button that refers to a mass of small-print boilerplate that hardly anyone can be expected to read. Or it may mean simply the failure to find and click on the button that says "I refuse consent." The advocates want something more demanding. Moreover, they don't want the cost of the decision to be too high. If insisting on privacy means exclusion from Google's search tool or Amazon's retail service, many proponents would view that as unfair. If Google or Amazon charged a price for not mining your data, many would call it extortion – like asking someone to pay in order not to be assaulted. So the idea of "consent" touches on deep and unresolved issues of entitlement to information.

Such issues have arisen in connection with employer-sponsored "wellness" programs that encourage employees to get check-ups that include a "health risk assessment" designed to generate prophylactic advice. At Pennsylvania State University such a program recently provoked a wave of privacy protests, apparently directed to parts of a questionnaire that addressed marital and job-related problems, among other things. The protesters also objected that the questionnaires would be analyzed by an "outside" consultant, even though the information would be subject to the confidentiality provisions of the federal Health Insurance Portability and Accountability Act. The University allowed people to refuse to participate subject to $100 per month premium surcharge.

No doubt such programs may be unnecessarily intrusive and may not safeguard information adequately, but the objections made in this case do not appear to have depended on such concerns. The $100 surcharge was based an estimate of the average additional health costs attributable to refusal to participate. The premise of the protests seems to have been that the interest in not disclosing this information even under substantial

safeguards is important enough that those who disclose should be asked to subsidize those who do not.

Social change often raises new questions about rights. When airplanes first appeared over people's homes, the question arose whether they were trespassing; when zoning codes limited what owners could build on their land, the question arose whether government had "taken" a portion of the individual's property, and was thus obliged to compensate them. More often than not, the law has refused to recognize claims of this sort. One reason has been fear that they would preclude many generally advantageous social practices. Another has been the belief that, except where the costs imposed by the practices cumulate visibly on particular individuals or groups, they are likely to even out over the long run. In a famous opinion declining to hold that a regulation of coal mining violated property rights, Justice Oliver Wendell Holmes spoke of an "average reciprocity of advantage" that over time obviated the need for individual compensation by distributing benefits evenly across the society.

The reciprocity theme occasionally surfaces in privacy discussion. Lanier's proposal to monetize data arises from a sense of injustice about the relative rewards to, on the one hand, data-mining entrepreneurs and high-tech knowledge workers, and on the other, the masses of people whose principal material endowment may be their control over their own personal information. In the health sector, doctors have been caught trying to derive patent rights from information embedded in their patients' DNA without informing the patients.

But privacy advocates rarely acknowledge the possibility that "average reciprocity of advantage" will obviate over time the need for individual compensation in some areas. Might it be the case, as with airplanes and zoning laws, that people will do better if individual data (anonymized where appropriate) is made freely available except where risks to individuals are unreasonably high or gains or losses are detectably concentrated? There will always be a risk that some data will be disclosed in harmful ways; for example when, personal data leaks out because of ineffective anonymization. However, the key question is whether we will

make a social judgment about what level of risk is reasonable or whether we shall accord property rights that allow each individual to make her own risk calculus with respect to her own data.

The latter approach would likely preclude valuable practices in ways analogous to what would happen if airlines had to get owners' consent for passing over private property. Moreover, strengthening rights in personal data could exacerbate, rather than mitigate, distributive fairness concerns. While it is surely unfair for doctors to earn large capital gains from DNA extracted without consent, wouldn't it also be unfair (admittedly in a lower key) for Freedom-Box-users to benefit from the Center for Disease Control's mining of Google searches for new viruses while denying access to their own internet searches?

The strong privacy position has disturbing implications for medical research. In the past, medicine has strongly separated research from treatment. Research is paradigmatically associated randomized control clinical trials. Treatment experience has been considered less useful to research because treatment records do not describe the condition of the patient or the nature of the intervention with enough specificity to permit rigorous comparisons. But information technology is removing this limitation, and, as the capacity to analyze treatment information rigorously increases, the quality of research could improve as its cost lowers.

However, this development is in some tension with expansive conceptions of privacy. A prominent group of bioethicists led by Ruth Faden of Johns Hopkins has argued that the emerging "learning health care system" will require a moral framework that "depart[s] in important respects from contemporary conceptions of clinical and research ethics." A key component of the framework is a newly recognized obligation on the part of patients to contribute to medical research. The obligation involves a duty to permit disclosure and use of anonymized treatment data for research purposes and perhaps also to undergo some unburdensome and non-invasive examination and testing required for research but not for individual treatment. (Anonymization is unlikely to be effective with data made

generally available on-line, but regimes involving selective and monitored disclosure have proven reliable.) The group justifies its proposal in terms of reciprocity values. Since everyone has a good prospect of benefiting from research, refusing to contribute to it is unfair free-riding.

Of course, the reciprocity idea assumes that researchers will make the fruits of the research derived from patient information freely available. People would be reluctant to agree to make a gift of their information if researchers could use it to make themselves rich. Effective constraints on such conduct should be feasible. Much medical research, including much of the highest value research, has been and continues to be done by salaried employees of charitable corporations.

Applied in this context, Lanier's proposal to monetize individual data looks unattractive. There's a danger that lots of valuable information would be withheld or that the costs of negotiating for it would divert a lot of resources from research and treatment. It is not clear what the resulting redistributive effects would be. Perhaps they would approximate a lottery in which the only winners would be a small number of people with little in common except that they happened to possess personal information that had high research value at the moment. At a point where we do not know who the winners will be, we would all be better off giving up our chances for a big payoff in return for assurance that we will have free access to valuable information. We can do this by treating the information as part of a common pool.

If it were the only way of transferring resources to the economically disadvantaged, monetization might be defensible as a social policy of desperation. But it seems a shabby and inefficient substitute for decent set of public institutions to discipline monopolistic power, provide public goods, and guarantee basic income, education, and health care. Astra Taylor agues compellingly in *The People's Platform* that techno-futurist discourse suffers from deep skepticism about public institutions. Yet, much of the current information techno-structure is a product of publicly initiated and supported research. There is no reason to

think that the capacities for creative innovation that the futurists celebrate cannot be applied effectively in the public realm.

The Panopticon metaphor emphasizes the undeniable dangers of domination in the new information technology. But there is also a promise of enhanced forms of social connection and collaboration. Bunkering into individualistic rights notions as a defense of traditional privacy risks stifling this potential.